CYBERSECURITY TIPS
SDPD Crime Prevention
August 2, 2016

CONTENTS

Because we as individuals and businesses rely on computers for nearly everything in our daily lives, we need to be aware of the risks of using them and take appropriate measures to minimize dangers. Among these dangers are viruses that erase or corrupt information in computers, viruses that infect computers and then propagate and infect other computers, hackers that break into computers and create mischief or steal information, employees who steal confidential business information, predators who attempt to meet and sexually exploit children, etc. This paper contains tips for protecting against malware, securing mobile devices, and using the Internet. Separate papers contain cybersecurity tips for businesses and parents.

The tips for businesses deal with physical protective measures, special measures for laptops, procedural and operational protective measures, personnel policies and employee training, malware protection, protecting bank accounts, using social media, cybersecurity planning, security for mobile devices, data privacy and security before, during, and after traveling with mobile devices, protecting corporate data in hotspots, safer use of the internet, preventing and dealing with data breaches, and due diligence when buying or merging with another business. It is

entitled *Cyber Security for Businesses* and can be opened on the Prevention Tips page of the SDPD website at **www.sandiego.gov/police/services/prevention/tips**.

The tips for parents deal with minimizing internet dangers, dangers of social networking, cyberbullying, reporting attempted sexual exploitation, preventing cyber crimes, use of home video games and Internet-connected toys, and protecting your child's identity. They are in a paper entitled *Child Safety and Security* that can also be opened on the Prevention Tips page of the SDPD website.

Finally, visit the FBI website at **www.fbi.gov/about-us/investigate/cyber** for more information about preventing cyber crime.

PROTECTING AGAINST MALWARE

Protecting Computers

Malware, which is short for malicious software, is computer code that's designed to disrupt computer operations, monitor and control online activity, or steal personal information. It includes the following:

- ***Viruses*** are programs that replicate themselves by infecting other programs. They often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing personal information, corrupting data, displaying political or humorous messages, spamming their contacts, or logging their keystrokes.
- ***Worms*** are standalone programs that replicate themselves in order to spread to other computers. Often, they use a computer network for this, relying on security failures on the target computer to access it. Unlike a computer virus, a worm does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
- ***Trojans*** are non-self-replicating programs containing malicious code that, when executed, carry out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. Trojans often employ a form of social engineering, presenting themselves as useful or interesting in order to persuade victims to install them on their computers.
- ***Scareware*** is a type of malware that is designed to trick victims into purchasing and downloading useless and potentially dangerous software. It usually appears as a pop-up that resembles Windows system messages and says that a large number of problems have been found on your computer and prompts you to buy software to fix the problems.
- ***Ransomware*** is a type of malware that restricts access to the infected computer system and demands a ransom paid to its creators to have the restriction removed.
- ***Spyware*** is software that gathers information about you, your computer, and your use of the Internet without your knowledge. It may also send that information to another entity or assert control over your computer.
- ***Adware*** is software that displays unwanted advertisements.

The following measures can help protect your computer from these dangers:

- Use strong passwords. Avoid using easily remembered numbers or available information like mother's maiden name, date of birth, hometown, names of relatives, ZIP code, phone number, etc. Passwords should have more than eight characters, with at least one capital letter, one lowercase letter, one number, and one symbol. Use of non-dictionary words or easily-remembered phrases is recommended, e.g. Johnhave3dawgs! Hackers can run a program that goes through the entire dictionary very quickly and crack any password which can be found in it. They can also use grammar rules to crack long passwords, especially those with pronouns. So use bad grammar and nouns. For maximum security you should use passwords that are at least 12 characters long, completely random, and have at least one capital letter, one lowercase letter, one number, and one symbol. Except for passwords created for one-time use, you should use different ones for each account or place. And change them every few months. You can test your passwords and get advice on creating strong ones at **www.passwordmeter.com**.
- Keep your computer up to date with the latest operating systems, applications, anti-virus (anti-malware) software and firewalls. The latter control incoming and outgoing network traffic based on an applied rule set. They

establish a barrier between a trusted, secure internal network and the Internet or another network that is assumed not to be secure and trusted. Use security software that updates automatically. Visit **www.OnGuardOnline.gov** for more information. This also applies to multi-function printers, fax machines, and copiers that can be accessed using a web browser.

- Don't open any e-mail from an unknown sender. Delete it without opening it. "Drive-by spam" can automatically download malware when an HTML e-mail is opened. You don't have to click on a link or open an attachment to get infected. Another way to prevent this kind of attack is to deactivate the display of HTML e-mails and display e-mails in pure-text format only.
- Use security software that updates automatically. Visit **www.OnGuardOnline.gov** for more information.
- Don't buy or download free anti-virus software in response to unexpected pop-ups or e-mails, especially ones that claim to have scanned your computer and detected malicious software.
- Make sure the pop-up blocker in the tools menu of your browser is turned on. This will prevent most pop-up ads. If you do get one, be careful in getting rid of it. Never click on any of its boxes. By clicking on No or Close you may actually be downloading malware onto your computer. And even clicking on the X in the upper right-hand corner can initiate a download instead of closing the advertisement. To be safe on a PC, hold down the Ctrl and Alt keys and hit Delete. Then in the Windows Security box click on Task Manger, and then click on End Task. This will clear your screen. Then run a full anti-virus scan.
- Don't click on the close buttons in video overlay ads on free live streaming websites. In a study published in 2016, researchers from Katholieke Universiteit Leuven in Belgium and Stony Brook University in the U.S. found that an average of 50 percent of the video overlay ads were malicious.
- Don't respond in any way to a telephone or e-mail warning that your computer has a virus even if it appears to come from an anti-virus software provider like Microsoft, Norton, or McAfee. "Helpful hackers" use this ploy to get you to download their software to fix the virus or sell you computer monitoring or security services to give them remote access to your computer so they can steal your passwords, online accounts, and other personal information. If you already have anti-virus software on your computer you'll receive a security update or warning directly on your computer.
- Turn off your computer and cover your webcam when you are not using them. The webcam can be controlled remotely if your computer has been compromised. Hackers have done this, captured nude photos of female victims, and threatened to release them publicly unless the victim agrees to send nude photos or videos, or engaged in a Skype session. This crime has been called sextortion. In it the hacker typically threatens to harm the victim's reputation by disclosing nude images.
- Use the latest versions of Internet browsers, e.g., Microsoft Internet Explorer 11, which is designed to prevent phishing attacks. Use Explorer in the "protected mode," which restricts the installation of files without the user's consent, and set the "Internet zone security" to high. That disables some of Explorer's less-secure features. And set your operating system and browser software to automatically download and install security patches.
- Don't install files or programs from CDs or flash drives before checking them for viruses.
- Scan demo disks from vendors, shareware, or freeware sources for viruses.
- Avoid using electronic bulletin boards.
- Don't download files from unknown sources.
- Don't allow any website to install software on your computers.
- Scan downloaded files for viruses. Avoid downloading executable files.
- In Technical Alert TA16-091A entitled *Ransomware and Recent Variants* dated March 31, 2016 the Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT) recommends that users and administrators take the following preventive measures to protect their computer networks from ransomware infections.
    - Employ a data backup and recovery plan for all critical information. Perform and test regular backups to limit the impact of data or system loss and to expedite the recovery process. Note that network-connected backups can also be affected by ransomware. Critical backups should be isolated from the network for optimum protection.
    - Use application whitelisting to help prevent malicious software and unapproved programs from running. Application whitelisting is one of the best security strategies as it allows only specified programs to run, while blocking all others, including malicious software.

- Keep your operating system and software up-to-date with the latest patches. Vulnerable applications and operating systems are the target of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.
- Maintain up-to-date anti-virus software, and scan all software downloaded from the Internet prior to executing.
- Restrict users' ability (permissions) to install and run unwanted software applications, and apply the principle of "Least Privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.
- Avoid enabling macros from e-mail attachments. If a user opens the attachment and enables macros, the embedded code will execute the malware on the machine. For enterprises or organizations it may be best to block e-mail messages with attachments from suspicious sources. For information on safely handling e-mail attachments see the US-CERT publication entitled *Recognizing and Avoiding Email Scams* at **www.us-cert.gov/sites/default/files/publications/emailscams_0905.pdf**. Follow safe practices when browsing the web. See Security Tip ST04-003 entitled *Good Security Habits* at **www.us-cert.gov/ncas/tips/ST04-003** and Security Tip ST06-008 entitled *Safeguarding Your Data* at **www.us-cert.gov/ncas/tips/ST06-008** for additional details.
- Do not follow unsolicited web links in e-mails. Refer to the US-CERT Security Tip ST04-014 entitled *Avoiding Social Engineering and Phishing Attacks* at **www.us-cert.gov/ncas/tips/ST04-014** or the US-CERT publication entitled *Ransomware* at **www.us-cert.gov/security-publications/Ransomware** for more information.

NIST Recommendations for System Patches and Malware Avoidance

The National Institute of Standards and Technology (NIST) publishes a series of computer security guides to help computer system managers protect their systems from hackers and malware. Vulnerabilities in software and firmware are the easiest ways to attack a system, and the two publications approach the problem by providing new guidance for software patching and malware avoidance.

A common method of avoiding attacks is to patch the vulnerabilities as soon as possible after the software company develops a patch, i.e., a piece of repair software for the problem. Patch management is the process of identifying, acquiring, installing, and verifying patches for products and systems. NIST's *Guide to Enterprise Patch* Management Technologies, Special Publication 800-40, Revision 3, July 2013, is available online at **http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf**. It is designed for agencies that take advantage of automated patch management systems such as those based on NIST's Security Content Automation Protocol (SCAP).

The second security document provides guidance to protect computer systems from malware, which is the most common external threat to most systems and can cause widespread damage and disruption. NIST's *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, Special Publication 800-83, Revision 1, July 2013, is available online at **http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf**. It provides information on how to modernize an organization's malware incident prevention measures and suggests enhancements to an organization's existing incident response capability to handle modern malware. It reflects the growing use of social engineering and the harvesting of social networking information for targeting attacks.

Protecting Mobile Devices

Cybercriminals are also targeting mobile devices with malware that compromises these devices. The Internet Crime Complaint Center (IC3), which is partnership between the FBI and the National White Collar Crime Center, suggests the following safety tips to protect them.

- When purchasing a smartphone, know the features of the device, including its default settings. Turn off features that are not needed to minimize the attack surface of the device.
- If the phone's operating system has encryption available, use it to protect your personal data in the case of loss or theft.

- With the growth of the application market for mobile devices, look at the reviews of the developer/company who published the application.
- Review and understand the permissions you give when you download applications. Understand their privacy and access setting. Be cautious in downloading applications and be aware of what data they access as a condition of their use. Look for comments other users post before downloading an application.
- Protect your device with a passcode. This is the first layer of physical security to protect its contents. Enable the screen lock feature after a few minutes of inactivity in conjunction with the passcode.
- Use biometrics such as fingerprint scanners as an alternative to complex passcodes.
- Obtain malware protection. Look for applications that specialize in anti-virus or file integrity that helps protect your device from rogue applications and malware.
- Be aware of applications that can track your location. They can be used by a criminal to assist a stalker or a burglar.
- Be aware that using jailbreak or rooting to remove certain restrictions imposed by the device manufacturer or cell phone carrier, which allows you nearly unregulated control over what programs can be installed and how the device can be used, often exploits significant security vulnerabilities and increases the attack surface of the device. Any time a user, application, or service runs in "unrestricted" or "system" level within an operational system, any compromise can take full control of the device.
- Don't allow your device to connect to unknown wireless networks. These networks could be rogue access points that capture information passed between your device and a legitimate server.
- If you decide to sell your device or trade it in, make sure you wipe the device (reset it to factory default) to avoid leaving personal data on the device.
- Install all smartphone updates to run applications and firmware. If you neglect this you risk having your device hacked or compromised.
- Avoid clicking on or otherwise downloading software or links from unknown sources.
- Use the same security precautions on your mobile phone as you would on your computer when using the Internet.

Smartphones continue to grow in popularity and are now as powerful and functional as many computers. To reduce their risk to security threats, the Federal Communications Commission (FCC) has published the following ten security tips. They are defined in detail at **www.fcc.gov/sites/default/files/smartphone_master_document.pdf**.

1. Set passcodes, i.e., Personal Identification Numbers (PINs), and passwords to prevent unauthorized access to your phone.
2. Don't modify your smartphone's security settings.
3. Back up and secure your data. These files can be stored on your computer or on removable storage card.
4. Only install apps from trusted sources. Before downloading one, conduct research to ensure it is legitimate.
5. Understand app permissions before accepting them. Check the privacy settings for each app before installing them.
6. Install security apps that enable remote location and wiping. These apps can also help you locate and recover your phone when you lose it.
7. Accept updates and patches to your smartphone's software. Keep your phone's operating system software up-to-date by enabling automatic updates or accepting updates when prompted from your service provider, operating system provider, device manufacturer, or application provider.
8. Be smart when using public Wi-Fi networks. Limit your use of public hotspots and instead use protected Wi-Fi from a network operator you trust.
9. Erase data off your old phone before you donate, resell, or recycle it.
10. Report a lost or stolen smartphone to the local law enforcement agency and then register it with your wireless provider.

Here are some tips for safe mobile banking:

- Use your wireless network when possible, not a Wi-Fi hot spot.
- Use Wi-Fi networks you know are secure.
- Make sure no one is looking over your shoulder to see your passwords.
- Know how to verify that a text message is from your bank. Your bank should tell you how to do this. This will

protect you from smishing, as discussed below under Internet Fraud and Other Crimes.

- Use your bank's app to connect, not a mobile web browser. The former should be equipped with the latest data-encryption technology.
- Log out when finished.
- Check your phone periodically for unfamiliar apps that could be malware.

The FCC has also designed a tool to help smartphone owners who aren't protected against mobile security threats. It can be seen at **www.fcc.gov/smartphone-security**. To use this tool choose your mobile operating system from the four listed and follow the ten steps above to secure your mobile device. More about the Smartphone security can be found at **www.fcc.gov/blog/fcc-and-public-private-partners-launch-smartphone-security-checker-help-consumers-protect-mobil**.

Wearable fitness devices have become very popular and it appears that criminal hackers are paying attention. Before you buy a wearable device or install a wearable app you should Google its name together with the words "hack," "fraud," and "scam." This will alert you to published problems and enable you to make a more informed purchasing decision. Then when you get a wearable device you should do the following.

- Set up your device and any associated online accounts with an obscure user name and a strong password.
- Read the privacy policy of any device and app you currently use or plan to use. Look closely at privacy assurances. Decide how serious you think the company is about protecting your data.
- Be prepared not to use certain features or apps if you do not feel the manufacturer is serious about security and could potentially expose sensitive information about you.
- Although these devices are not easily hacked, it is possible for a hacker to guess your PIN by recording the motion of the hand you use to when typing your PIN on a keypad. To be safe you should not use the arm with the device when typing in a PIN.

SECURING MOBILE DEVICES

Smartphones, tablets, and other mobile devices are now as powerful and functional as many computers. Therefore is necessary to protect them just like you protect your computer or laptop. US-CERT provides the following tips to safeguard your personal information:

- Lock your device when you're not using it. Even if you only step away for a few minutes, it's enough time for someone else to steal or destroy information in it.
- Disconnect your device from the Internet when you aren't using it. The likelihood that attackers or viruses scanning the network for available devices will target you becomes much higher if your device is always connected.
- Keep security software up to date. Update security patches so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. Install them.
- Consider creating separate user accounts. If multiple people are using the device, someone else may accidentally access, modify, or delete your information. If you have the option, create different user accounts for each user and set the access and privileges for each account.
- Establish guidelines for usage. If multiple people using your device, especially children, make sure they understand how to use the device safely. Setting boundaries and guidelines will help protect your data.
- Back up your data. Whether or not you take steps to protect yourself, there will always be a possibility that something will happen to destroy your data. Regularly backing it up reduces the stress and consequences that result from losing important information.

US-CERT published the following revised tips on cybersecurity for electronic devices in ST05-017 on Dec. 22, 2015.

- Remember physical security. Having physical access to a device makes it easier for an attacker to extract or corrupt information. Do not leave your device unattended in public or easily accessible areas. See ST04-017 entitled *Protecting Portable Devices: Physical Security* for more information.

- Keep software up to date. If the vendor releases updates for the software operating your device, install them as soon as possible. Installing them will prevent attackers from being able to take advantage of known problems or vulnerabilities. See ST04-006 entitled *Understanding Patches* for more information.
- Use strong passwords. Choose devices that allow you to protect your information with passwords. Select passwords that will be difficult for thieves to guess, and use different passwords for different programs and devices. Do not choose options that allow your computer to remember your passwords. See ST04-002 entitled *Choosing and Protecting Passwords* for more information.
- Disable remote connectivity. Some mobile devices are equipped with wireless technologies, such as Bluetooth, that can be used to connect to other devices or computers. You should disable these features when they are not in use. See ST05-015 entitled *Understanding Bluetooth Technology* for more information
- Encrypt files. If you are storing personal or corporate information, see if your device offers the option to encrypt the files. By encrypting files, you ensure that unauthorized people can't view data even if they can physically access it. When you use encryption, it is important to remember your passwords and passphrases; if you forget or lose them, you may lose your data.
- Be cautious of public Wi-Fi networks. Before you connect to any public wireless hotspot like on an airplane or in an airport, hotel, train/bus station or café:
    - Be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate.
    - Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network.
    - Only use sites that begin with **https://** when doing online shopping or banking. Using your mobile network connection is generally more secure than using a public wireless network.

Wi-Fi Hacking and Hotspot Dangers

Use of Wi-Fi in coffee shops, libraries, airports, hotels, universities, and other public places pose major security risks. While convenient, they're often not secure. You're sharing the network with strangers, and some of them may be interested in your personal information. If the hotspot doesn't require a password, it's not secure. If it asks for a password through your browser simply to grant access, or it asks for a Wired Equivalent Privacy (WEP) password, it's best to treat it as unsecured. You can be more confident that a hotspot is secure only if it asks for the Wi-Fi Protected Access (WPA and WPA2) password. WPA2 is more secure. However, a flaw in a feature added to Wi-Fi called Wi-Fi Protected Setup (WPS) allows WPA and WPA2 security to be bypassed and broken by brute force in many situations.

Also, unsecure laptops and smartphones make it easy for a hacker to intercept information to and from the web, including passwords and credit- or debit-card numbers. They are also vulnerable to malware infections, and to having their contents stolen or destroyed. A hacked laptop or smartphone can also create a security risk for the user's workplace if it contains a password to the corporate network. Wi-Fi users should take the following steps to reduce these risks:

- Turn the Wi-Fi on your laptop, PDA, and smartphone off when you aren't using the network. Otherwise your Wi-Fi card will broadcast your Service Set Identifier (SSID) looking for all networks it was previously connected to. This enables hackers to figure out the key that unscrambles the network password.
- Use a known service instead of Free Public Wi-Fi or similar risky, unknown signals called ad hoc networks.
- Check the Wi-Fi security policies of your service provider and install the protections they offer to ensure it's a known network and not an "evil twin" hacker site pretending to be the legitimate one.
- Pay attention to warnings that a Secure Sockets Layer (SSL) certificate is not valid. Never accept an invalid certificate on a public wireless network. Log off and look for a trustworthy network. Look for the padlock indicating an SSL connection. Keep your firewall on. And keep your operating system updated.
- Find out if your company offers a Virtual Private Network (VPN) and learn how to use it. Encrypted VPN sessions offer the highest security for public wireless use. Use Hypertext Transfer Protocol Secure (HTTPS) when accessing a website or use a VPN to protect the transmission of sensitive information when using a wireless connection.
- Upgrade your Wi-Fi cards. The older WEP security is easily hacked. The new WPA and WPA2 are much more resistant to attack.

- Secure IEEE 802.11 wireless access points with a WPA2 and Advanced Encryption Standard (AES) encryption to protect sensitive communications.
- If your router has the WPS function, disable it. Methods have been published for doing this for some models. But on others, disabling the WPS in the user interface is not effective and the device remains vulnerable to attack.
- Learn to connect securely. Even the vulnerable WEP offers more privacy and protection than an unsecured public connection. It's not something the average hacker can crack. Look at your connection page for a name and description. A legitimate wireless network is simply called a "wireless network." It will display an icon of just one connected computer. So called ad hoc or peer-to-peer networks that are used by scammers to steal your personal information scammers are not legitimate. The will be called "computer-to-computer" networks and display an icon of several computers connected together. Never connect to this network. And be sure to set up your computer so it doesn't automatically connect to a network but allows you to choose a connection.
- Only log in or send personal information on secure website pages, i.e., ones that are encrypted. They will have **https://** or **shttp://** in the Uniform Resource Locator (URL) and a "lock icon" at the top or bottom of your browser window. You can click on this icon to display information about the website and help you verify that it's not a fake.
- Use a unique, strong password for each account.
- When you've finished using an account, log out. Don't stay signed in.
- Pay attention to warnings from your browser if you try to visit a fake website or download a malicious program.
- Remove all passwords and browsing history after using a shared computer.
- Disable file-sharing on your laptop.
- Don't send any sensitive personal or business information while in a hotspot unless you absolutely have to.
- Put a strong password on your wireless network.
- In shopping, it's fine to browse website when you're out but wait until you are at home to do any online business.
- Be aware of the existence of malware that enables a mobile device to be used as an open microphone with or without the owner's knowledge.

How to Prevent Theft of Your Device

The theft of wireless devices, particularly smartphones, is sharply on the rise across the country. The high resale value of these devices has made them a prime target for robbers. And the personal information contained on them is very attractive to identity thieves. Things you can take to protect yourself, your device and the data it contains, along with things to if your device is stolen or lost are listed below.

- Pay attention to your surroundings when using your device in public. Don't focus on your device and don't use it if someone might grab it and run. If it's not urgent that you use your device, wait until you're in a secure and private place to do so.
- Don't let anyone "borrow" your device. If a stranger wants to make a call, offer to make it for him or her.
- Never leave your device unattended in a public place. And don't leave it visible in an unattended vehicle. Lock it in the glove compartment when you park, or in the trunk before you park.
- Never leave your device out in the open where it is easy to steal, e.g., in your back pocket. Keep it where it's harder to reach, e.g., in an inside pocket of your jacket.
- If you carry your device in a purse, use one with a shoulder strap. Keep the strap over your shoulder, the flap next to your body, and your hand on the strap. Hang the purse diagonally across your body and secure the flap.
- Record the device's make, model number, serial number, and unique identification number, i.e., either the International Mobile Equipment Identifier (IMEI) or the Mobile Equipment Identifier (MEID) number. Keep them in a safe place. The police may need this information if the device is stolen or lost.
- Review your warranty or service agreement to find out what will happen if your device is stolen or lost. Consider buying insurance if the policy is not satisfactory.

How to Protect the Data on Your Device

- Establish a strong password to restrict access. This will help protect you from unwanted usage charges and misuse of your personal data if your device is stolen or lost.
- Install and maintain anti-theft software if your phone doesn't have a kill switch. Apps are available that will:
  - Locate the device from any computer.
  - Lock the device to restrict access.
  - Wipe sensitive data from the device, including contacts, text messages, photos, e-mails, browser histories, and user accounts such as Facebook and Twitter.
  - Make the device emit an alarm to help the police locate it.
- Display contact information such as an e-mail address or phone number on your lock screen so that the device can be returned to you if it is lost and found. But don't include sensitive personal information such as your home address.
- Be careful about storing personal information on your device. Social networking and other apps may allow unwanted access to it.
- Back it up on your personal computer or other back-up device.
- Keep a list of all apps you have on your smartphone.
- See the section below on data privacy and security when traveling on business with mobile devices.

What to Do If Your Device Is Stolen

- Report the theft to the police as soon as possible. Include the make and model, and serial and IMEI or MEID numbers. Some carriers require proof that the device was stolen. A police report will provide that documentation.
- If you aren't sure certain whether your device was stolen or simply misplaced, attempt to locate it by calling it or by using its anti-theft software's Global Positioning System (GPS) locator. Even if you have only lost it, you should remotely lock it to be safe.
- If your device has anti-theft software, use it to lock the device, wipe sensitive information, and/or activate the alarm. Note that under California Business and Professions Code Sec. 22761 any smartphone manufactured on or after July 1, 2015, and sold in California after that date, shall include a technological solution, commonly referred to as a kill switch, at the time of sale, to be provided by the manufacturer or operating system provider, that, once initiated and successfully communicated to the smartphone, can render the essential features of the smartphone inoperable to an unauthorized user when the smartphone is not in the possession of an authorized user. The essential features are defined as ability to use the smartphone for voice communications, text messaging, and the ability to browse the Internet, including the ability to access and use mobile software applications. Use of a kill switch will make your phone useless to thieves.
- Report the theft or loss to your carrier. You will only be responsible for charges incurred prior to when your report. If you provide your carrier with the IMEI or MEID number, your carrier may be able to disable your device and block access to the information it carries. Request written confirmation from your carrier that you reported the device as missing and that the device was disabled.
- Notify financial companies you have accessed with your device. Put banks and credit card companies on alert regarding your stolen or lost device and cancel their cards to prevent fraudulent transactions on your accounts.
- Change your passwords for all e-mail, banking, and social networking accounts that you have accessed with your device.
- Call ecoATM at **(858) 255-4111** to ask if your device has been sold in one of its kiosks. You will need a police report for it to investigate the theft.

SECURING YOUR HOME NETWORK

Home routers have become an integral part of our global communications footprint as use of the Internet has grown to include home-based businesses, telework, schoolwork, social networking, entertainment, and personal financial management. Routers facilitate this broadened connectivity. Most of these devices are preconfigured at the factory and are Internet-ready for immediate use. After installing routers users often connect immediately to the Internet without performing any additional configuration. Users may be unwilling to add configuration safeguards because configuration seems too difficult or users are reluctant to spend the time with advanced configuration settings.

Unfortunately, the default configuration of most home routers offers little security and leaves home networks vulnerable to attack. Small businesses and organizations often use these same home routers to connect to the Internet without implementing additional security precautions and expose their organizations to attack.

Home routers are directly accessible from the Internet, are easily discoverable, are usually continuously powered-on, and are frequently vulnerable because of their default configuration. These characteristics offer an intruder the perfect target to obtain a user's personal or business data. The wireless features incorporated into many of these devices add another vulnerable target. You can you prevent unauthorized access to your home network by following the steps listed below that are designed to increase the security of home routers and reduce the vulnerability of the internal network against attacks from external sources.

- Change the default username and password. These are readily available in different publications and are well known to attackers. Manufacturers set them at the factory for their troubleshooting convenience. They should be changed immediately during the initial router installation. It's best to use strong passwords that are at least 12 characters long, completely random, and have at least one capital letter, one lowercase letter, one number, and one symbol. Passwords should be changed every at least every 90 days.
- Change the default SSID. This is a unique name that identifies a particular wireless local area network (WLAN). All wireless devices on a WLAN must use the same SSID to communicate with each other. Manufacturers set a default SSID at the factory. This SSID typically identifies the manufacturer or the actual device. An attacker can use the default SSID to identify the device and exploit any of its known vulnerabilities. Users sometimes set the SSID to a name that reveals their organization, location, or own name. This information makes it easier for the attacker to identify the specific business or home network. Using default or well-known SSIDs also makes brute force attacks against WPA2 keys easier. Choose an SSID that is unique and not tied to your personal or business identity.
- Don't stay logged into the management website for your router. Routers usually provide a website so users can configure and manage the router. Do not stay logged into it as a defense against Cross-Site Request Forgery (CSRF) attacks. In this context, a CSRF attack would transmit unauthorized commands from an attacker to the router's management website.
- Use WPA2 with AES for data confidentiality. Some home routers still use WEP, which is easily hacked. If your router or device only supports WEP you should upgrade it or configure it with the 128-bit key option and the longest pre-shared key the router administrator can manage. The newer standard, WPA2 with AES, encrypts the communication between the wireless router and the wireless computing device thus providing stronger authentication and authorization between the devices. It is the most secure router configuration for home use and incorporates 128-bit encryption that is encouraged by NIST.
- Disable WPS immediately. It provides simplified mechanisms to configure moderately secure wireless networks. A design flaw in it for the PIN authentication significantly reduces the time required to determine the entire PIN because it allows an attacker to know when the first half of the 8-digit PIN is correct. The lack of a proper lockout policy after a certain number of failed attempts to guess the PIN on many wireless routers makes a brute-force attack much more likely to occur.
- Limit WLAN signal emissions. WLAN signals are frequently broadcasted beyond your home. This allows eavesdropping by intruders outside your network perimeter. Therefore it's important to consider antenna placement, type, and transmission power levels to limit the broadcast coverage area when securing your WLAN. If possible, use a directional antenna to restrict WLAN coverage only to the areas needed. Experimenting with transmission levels and signal strength will also allow you to better control WLAN coverage. Note that an attacker with a sensitive antenna may still be able to eavesdrop on your network.
- Turn the network off when it is not being used. This may be impractical if it occurs frequently, but it should be considered for extended offline periods. Then outside attackers will be unable to exploit your WLAN.
- Disable Universal Plug and Play (UPnP) when it is not needed. This feature allows networked devices to seamlessly discover and establish communication with each other on the network. Though it eases initial network configuration, it is also a security hazard. For example, malware within your network could use UPnP to open a hole in your router firewall to let intruders in. Thus it should be disabled unless you have a specific need for it.
- Upgrade router firmware. Just like software on your computers, the router firmware, i.e., the software that operates it, must have current updates and patches. Many of the updates address security vulnerabilities that could affect the network. When considering a router, check the manufacturer's website to see if it provides updates to address security vulnerabilities.

- Disable remote management. This will keep intruders from establishing a connection with the router and its configuration through the Wide Area Network (WAN) interface.
- Monitor network for unknown device connections. Use your router's management website to determine if any unauthorized devices have joined or attempted to join your network. If an unknown device is identified, a firewall or Media Access Control (MAC) filtering rule can be applied on the router. See the literature provided by the manufacturer or the manufacturer's website for further information on how to apply these rules.

INTERNET FRAUD AND OTHER CRIMES

In 2015 the IC3 received nearly 290,000 consumer complaints on its website. About 44 percent of these complaints reported financial losses. The total reported loss from these was about $1 billion. You may be at risk if you answer "yes" to any of the following questions:

- Do you visit websites by clicking on links within an e-mail?
- Do you reply to e-mails from persons or businesses you are not familiar with?
- Have you received packages to hold or ship to someone you met on the Internet?
- Have you been asked to cash checks and wire funds to someone you met on the Internet?
- Would you cash checks or money orders received through an Internet transaction without first confirming their legitimacy?
- Would you provide your personal banking information in response to an e-mail notification?

If you become a victim of Internet fraud or receive any suspicious e-mails you should file a complaint with the IC3 at **www.ic3.gov**. Its website also includes press releases on the latest scams and other Internet dangers, and tips to assist you avoiding a variety of Internet frauds. You should also contact your e-mail provider. Most keep track of scams. Send your provider the suspicious message header and complete text.

The following material deals with several specific kinds on Internet fraud and other crimes: e-mail scams, online shopping frauds, phishing, spear phishing, smishing, vishing, whaling, social network dangers, fake websites, e-card dangers, and unsafe drugs from online pharmacies.

E-mail Scams

Cybercriminals use e-mail in many clever ways to try to take your money and identity, and disrupt your computer operation, gather sensitive information, or gain unauthorized access to your computer. To protect your assets and computer you should never reply, click on any links, or open any attachments of e-mails that offer great bargains or something that's not legal. If you want to click on a link, check the URL first by hovering over it, not clicking, to see if the destination name matches the URL exactly. If it doesn't, it's a scam designed to take you to a fake website. And if you don't recognize the sender, you should delete the e-mail without even opening it. Be especially suspicious about the following:

- Business opportunities to make money with little effort or cash outlay
- Offers to sell lists of e-mail addresses or software
- Any offer that asks for an immediate response
- Chain letters
- Work-at-home schemes
- Health and diet claims of scientific breakthroughs, miraculous cures, etc.
- Get-rich-quick schemes
- Free goods offered to fee-paying group members
- Investments promising high rates of return with no risk
- Kits to unscramble cable TV signals
- Guaranteed loans or credit on easy terms
- Credit repair schemes
- Vacation prize promotions
- Renew magazine or newspaper subscriptions

- Special offers that require a credit check and a small fee for verification expenses to be paid by a credit or debit card
- Notices of prize or lottery winnings that require you to pay a fee to cover expenses
- Offers to enroll you in a health insurance plan under the ACA, commonly called Obamacare
- Requests for personal or financial information

Regarding the latter, cybercriminals often pose as government agencies or financial institutions that you normally deal with. Remember that government agencies never send important things by e-mail and your financial institutions already have your personal information.

If you suspect something might be a scam, check it out on Hoaxslayer at **www.hoax-slayer.com**. This website is devoted to debunking e-mail hoaxes and exposing Internet scams. It is constantly increasing its compiled list of scams. Regarding chain letters, US-CERT recommends being especially cautious if the e-mail has any of the following characteristics:

- Suggests tragic consequences for not performing some action
- Promises money or gift certificates for performing some action
- Offers instructions or attachments claiming to protect you from a virus that is undetected by anti-virus software
- Claims it's not a hoax
- Includes multiple spelling or grammatical errors, or the logic is contradictory
- Urges you to forward the message

If an e-mail looks suspicious, it is always best to err on the side of caution and delete the message or mark it as junk mail. And as always, think before you act and be wary of any communication that asks you to act immediately, requests personal information, or just sounds too good to be true.

Online Shopping Frauds

If you use a credit card the federal Truth in Lending Act limits your liability to $50 for any unauthorized or fraudulent charges made before you report the billing error. To protect yourself you need to write to your credit card company within 60 days after the date of the statement with the error and tell it: (1) your name and account number, (2) that your bill contains an error and why it is wrong, and (3) the date and amount of the error. You need to pay all other charges but not the disputed amounts.

Don't use a bank debit card when shopping online, especially on an unfamiliar website. If something goes wrong your account can be emptied quickly without your knowledge. This can result in overdrafts, fees, and an inability to pay your bills. The federal Electronic Funds Transfer Act provides some liability protection in the event of any fraudulent charges resulting from the loss or theft of your card, or your card data. In the latter case you would not be liable for any fraud charges if you report them within 60 days after you receive your bank statement. But even then your bank is not obligated to restore your funds for at least two weeks while it investigates. But if you fail to report the fraud charges within 60 days of receiving your bank statement there is no limit on your liability. So if have to use a debit card, use one that is reloadable. Then you only risk the amount you put on the card if something goes wrong.

Consumers should be aware that if a deal looks too good to be true, it probably is. In one scam the victim located a car on the Auto Trader website and contacted the seller directly by e-mail. He was told that the car would be shipped to him for inspection and approval if he wired the money to a bank account where it would be held in escrow. He wired the money but the car never arrived. To prevent this kind of scam consumers need to be diligent in verifying all the parties involved in the purchase by phone calls, face-to-face meetings, etc. In a similar case the consumer asked to see the car before wiring any money. The scammer ended all contacts at that point.

Another example involved a Craigslist ad for a vacation apartment rental in New York City. The renter was told he had to act fast and wire the money or he'd lose out on this good deal. All three elements of a typical scam were present in this case: (1) act fast or lose the deal, (2) wire the money, and (3) a price that was too good to be true. Scammers also use Craigslist and other websites to advertise rentals in your area. They will make a duplicate of a

legitimate ad but with a much lower price and a different contact number. They will ask for cash upfront without showing the property or ask you to fill out an application with your Social Security Number (SSN) or other personal information. These are signs of the scam.

Online scams also promise great deals on airline tickets, timeshare properties, and vacation packages. The biggest red flag is when payment is requested by a wire transfer. It's difficult to track these transfers and almost impossible to get a refund. Check out the company offering the deal before making a purchase. If it and the deal appear to be legitimate, pay by credit card and not by wire. Then if the deal turns out to be fraudulent, you can dispute the charges as indicated above.

Phishing

In this e-mail scam identity thieves fish for personal information by sending realistic-looking e-mails that ask recipients to go to a bogus website and to verify their credit card number, password, Personal Identification Number (PIN), or other account information. Legitimate banks and financial institutions don't send e-mails asking you to verify your account information. They already have it. The following are examples of scammers posing as the IRS, FBI, Federal Deposit Insurance Corporation (FDIC), and the Centers for Disease Control and Prevention (CDC).

Each year during tax preparation time there is a surge in the number of frauds by criminals posing as IRS officials to obtain personal information for identity theft. The IRS never sends out unsolicited e-mails or asks for detailed personal or financial information. Neither does it say you are entitled to a refund and you can get it by clicking on a link to a website and sending your personal information. Any such e-mails are frauds. Some phone calls from someone stating they are from the IRS may also be frauds. If you are suspicious, contact the IRS at **(800) 829-1040** to find out if it has a legitimate need to contact you. Go to the IRS website at **www.irs.gov** for information on the latest scams and instructions on how to protect yourself from suspicious e-mails or phishing schemes. Beware of any websites claiming to be from the IRS that end in .**com**, **.net**, **.org**, etc. The IRS also recommends forwarding the suspicious e-mail to it at **phishing@irs.gov**.

The growing popularity of tax preparation software has led to a rise in e-mail scams targeted at do-it-yourself taxpayers. The fraudulent e-mails claim to come from a software provider and might offer a software update or download. They may ask for personal financial information or other sensitive data and contain links to websites that could download malware. Legitimate software providers routinely send customers e-mails advising them of the status of their tax returns but never ask for sensitive personal data. Any software updates should be done on your provider's website or desktop product. Also, forward any suspicious e-mails to your software provider's security center.

Fraudulent e-mails have also been sent out by criminals posing as FBI agents and officials. They give the appearance of legitimacy by using the FBI seal, letterhead, and pictures of the FBI Director. They may also claim to come from the FBI's domestic or overseas offices. Like the IRS, the FBI does not send out e-mails soliciting personal or financial information. For more information on this kind of fraud go to the FBI website at **www.fbi.gov** and click on New E-Scams and Warnings under Be Crime Smart.

Another agency that has become aware of fraudulent e-mails in its name is the FDIC. These ask recipients to "visit the official FDIC website" by clicking on a hyperlink that directs them to a fake website that includes hyperlinks that open a "personal FDIC insurance file" to check on their deposit insurance coverage. Clicking on these links will download a file that contains malicious software to collect personal and confidential information.

In 2009 the CDC issued a health alert warning people not to respond to an e-mail referencing a CDC-sponsored state vaccination program for the H1N1 (Swine Flu) contagion that requires registration on "www.cdc.gov." People that click on this embedded link risk having a malicious code installed on their computer. Examples of this and other hoaxes and rumors can be seen at **www.cdc.gov/hoaxes_rumors.html**.

In April 2014 the San Diego Superior Court alerted the public about a new scam involving unsolicited e-mails claiming to be from the court. One person who had an issue before the court received an attachment with the e-mail. That person opened the attachment and soon discovered it contained a virus. The Court reiterated to the public that

it does not communicate with people with issues before the court by unsolicited e-mail or telephone. It also does not communicate regarding "missed jury duty" or cases of which you are unaware. You should delete these e-mails or disregard these phone calls.

A scam that's rampant during the holiday season involves e-mails that ask you to confirm an online purchase order or a package shipment by clicking an included link or attachment. This is done to trick you into giving up control over their computers and identities.

In summary, phishing e-mails usually look like they come from a government office or a company that you do business with and contain threats of problems that will occur if you don't comply with its instructions and click on an enclosed link or attachment. They often have spelling and grammatical errors. So read each e-mail carefully. If you suspect it might be a fake, contact the office or company and ask if it is legitimate. When in doubt, delete it. If you feel you might have been tricked and fear the consequences, file a report with the Federal Trade Commission (FTC) at **www.ftc.gov/complaint**.

Here are some specific tips to use in countering phishing:

- Don't open any e-mail from an unknown sender, especially if it offers something sensational, e.g., a video of Osama Bin Laden's death. Delete it without opening it. "Drive-by spam" can automatically download malware when an HTML e-mail is opened. You don't have to click on a link or open an attachment to get infected. Another way to prevent this kind of attack is to deactivate the display of HTML e-mails and display e-mails in pure-text format only.
- Don't open any unexpected e-mail attachments.
- Don't give out any passwords or personal information or click on any links no matter what the e-mail says, e.g., that you will be locked out of your account if you don't provide the information, or that you owe money.
- Don't click on links in e-mail messages purporting to come from your bank or any other institution or business that you have an account with. Retype the address into your browser. If you do click on a link and are prompted to log in with your password, don't do it. Close your browser and log into your account to make a payment or do whatever the message said.
- Don't click on any links in unsolicited e-mails you receive from companies you do business with, e.g., from FedEx regarding an "undeliverable" package.
- Don't click on any links in e-mail messages from a friend or person you know unless the message states why the link is being sent specifically to you and you recognize the URL of the link as one that the person might send you. Often someone hacks into an e-mail account and sends a message to everyone in the address book with a link to a fake or malicious website. You should delete such e-mails and send your friend an e-mail about it. Friends then usually send a message to everyone in their address books saying "I've been hacked. Don't click on any links."
- Don't double click on any Internet pop-up with a link to an offer or provide any personal information in response to a pop-up offer. And never enter personal information on a pop-up page.
- Use the latest versions of Internet browsers, e.g., Microsoft Internet Explorer 11, which is designed to help protect against socially-engineered malware. Use Explorer in the "protected mode," which restricts the installation of files without the user's consent, and set the "Internet zone security" to high. That disables some of Explorer's less-secure features. And set your operating system and browser software to automatically download and install security patches.
- Make sure the website page you are entering sensitive information on is secure. You can tell it is secure when the address on the top of your screen where the URL is displayed begins with **https://** rather than **http://.** You can also look for a closed padlock or an unbroken key on the bottom of your screen to indicate the page is secure. If the lock is open the site or the key is broken, the page is not secure. Note that on many websites only the order page will be secure.
- Read the website's privacy policy. It should explain what personal information it collects, how the information is used, whether it is provided to third parties, and what security measures are used to protect the information. Consider taking your business elsewhere if you don't see, understand, or agree with the policy.
- Keep your computer up to date with the latest operating systems, applications, anti-virus software and firewalls. Use security software that updates automatically. Visit **www.OnGuardOnline.gov** for more information.

- Don't buy or download free anti-virus software in response to unexpected pop-ups or e-mails, especially ones that claim to have scanned your computer and detected viruses.
- Make sure the pop-up blocker in the tools menu of your browser is turned on. This will prevent most pop-up ads. If you do get one, be careful in getting rid of it. Never click on any of its boxes. By clicking on No or Close you may actually be downloading malware onto your computer. And even clicking on the X in the upper right-hand corner can initiate a download instead of closing the pop-up. To be safe on a PC, hold down the Ctrl and Alt keys and hit Delete. Then in the Windows Security box click on Task Manger, and then click on End Task. This will clear your screen. Then run a full computer security scan.
- Don't respond in any way to a telephone or e-mail warning that your computer has a virus even if it appears to come from an anti-virus software provider like Microsoft, Norton, or McAfee. "Helpful hackers" use this ploy to get you to download their software to fix the virus or sell you computer monitoring or security services to give them remote access to your computer so they can steal your passwords, online accounts, and other personal information. If you already have anti-virus software on your computer you'll receive a security update or warning directly on your computer.
- Look for valid trust marks to increase your confidence in using a website. Reputation trust marks like BBBOnline offer a basic level of proof that there is an actual business behind the website and that it follows proper business practices. Privacy trust marks like TRUSTe indicate that the business is aware of identity theft and personal data abuse and abides by the requirements of the trust mark provider in its privacy policy. A Secure Socket Layer (SSL) trust mark like VeriSign indicates that the site uses up-to-date encryption technology to scramble communications between the website and your computer. And security-scanning trust marks like McAfee SECURE indicate that the business uses a regularly scheduled security auditing service for its website to ensure that it is free of malware. Because a phisher could create a false trust mark and verification website, you cannot know that the mark is valid unless you click on it. A link will take you to the verification website of the trust mark provider. The trust mark is valid if its verification website has **https://** in its URL.
- Be careful in visiting websites that don't have trust marks.

Spear Phishing

This is a more sophisticated version of phishing. It targets groups of people who have something in common, e.g., they work for the same company, deal with the same financial institution, or attend the same college. The fraudulent e-mails appear to come from organizations the potential victims would normally get e-mails from. Success in spear phishing depends on three things: (1) the apparent source of the e-mail must be a known and trusted individual or organization, (2) there is information in the e-mail that makes it look legitimate, and (3) the request for personal or company-privileged information, or direction to click on an included link must have a logical basis, e.g., to update usernames and passwords. The information needed for these things is obtained by hacking into the organization's computer network, data breaches, or combing through other websites, blogs, and social networking sites.

Spear-phishing attacks are often used by individuals conducting targeted, rather than opportunistic, attacks. Those responsible for the attack may be seeking precise information stored on an organization's network or systems rather than monetary gain. Every organization is at risk of being the target of a spear-phishing attack. The success of these attacks depends on finding the weakest link in a corporate network. This is usually one person who falls for an authentic-looking e-mail. Thus, the company's employees need to be the first line of defense. Here are some things they should do to avoid becoming a spear-phishing victim and causing great harm to their company.

- Always treat unsolicited or unexpected e-mail containing attachments or links with caution, especially when the e-mail appears related to known events or projects.
- Remember that most companies, banks, agencies, etc. don't request personal information by e-mail. If in doubt, call the sender. But don't use the number in the e-mail. It's usually phony too.
- Use a browser with a phishing filter.
- Never open an attachment or follow a link from a suspicious e-mail to another website. Look up the URL and enter it manually.
- Never respond to a request to verify passwords.
- Become paranoid about e-mail.
- Report any suspicious e-mail to your company's Information Technology (IT) manager in accordance with its security policy. Also report this activity to the IC3 by filing a complaint at **www.ic3.gov**.

Spear phishing can best be mitigated at the company level with increased cybersecurity. When weighing available options for mitigation strategies, companies should begin by asking themselves what the current and future consequences would be if proprietary data, personally-identifiable information, research and development-related data, e-mail, or other critical information were stolen. The answers will define what the company should protect.

Companies should also try to protect their employees from receiving malicious e-mail. With access to all incoming e-mail and knowledge of the kinds of e-mail that each employee normally receives, a cybersecurity system could recognize unusual e-mail and warn employees of it, especially before significant events and meetings. It should also warn employees about social engineering and spear phishing related to these events and meetings. And it should measure expected network activity levels so that changes in patterns can be more easily identified.

Smishing

This is phishing with text messages instead of e-mails. "Smishing" is a term coined from Short Message Service (SMS) and phishing. In these scams you may receive a SMS stating that your account will be charged for some particular program or purchase unless you visit a given URL within two days to cancel the order. When you click on the cancel link you will download malware to your computer. Don't respond to these SMSs. Alternatively, the SMS may give you a phone number to call where you will be asked for personal information. Before calling verify that the number matches the number of the named institution, e.g., your bank. And never give out personal information unless you have initiated the call.

Vishing

In this scam criminals use Voice over Internet Protocol (VoIP) technology to make telephone calls from anywhere in the world pretending to be a legitimate business, often using a fraudulent called ID matching the identity of the misrepresented company. The term "vishing" comes from voice phishing. It directs recipients to call a telephone number where they are tricked into giving up personal financial information. They might receive an urgent recorded message telling them that their credit card has been compromised and directing them to call the following telephone number immediately and punch in their 16-digit account number to verify their identity. Alternatively, you may receive an e-mail asking you to call a particular number to prevent your account from being blocked. Someone there will attempt to get you to give up personal information. The best defense against vishing is to treat any unsolicited telephone message with suspicion and only give your personal information out when you have initiated the call and are sure the other party is legitimate.

Whaling

In another scam known as "whaling," hackers will pose as a trusted source and send fake e-mails to high-ranking executives to gain sensitive information or trick them into clicking on a link that takes them to a website that downloads software that secretly records keystrokes and sends data to a remote computer over the Internet. This lets the criminal capture passwords and other personal or corporate information, and gain control of the executive's computer. In one case fake subpoenas have been sent to executives commanding them to appear before a grand jury in a civil case. The link that offers a copy of the entire subpoena downloads the malicious software.

Social Networking Dangers

Malware creators, identity thieves, burglars, and spammers are increasingly targeting users of social networking sites in an effort to steal personal data and account passwords. One of the tactics they use to gain access to this information involves sending social networking users e-mails that appear to come from online friends. For example, some Facebook users have been receiving e-mails from their "friends" that claim to contain a video of them. When they click on it they download malware that installs a malicious program on their hard drive. A virus known as Koobface sends itself to all the friends on the victim's Facebook profile. A new version of the virus also is affecting users of Myspace and other social networking sites. Cyber-criminals are tricking social networking users into downloading malicious software by creating fake profiles of friends, celebrities, and others. Security experts say that such attacks, which became widespread in 2008, are increasingly successful because more and more people are becoming comfortable with putting all kinds of personal information about themselves on social networking sites.

They warn that users need to be very careful about what information they post because it can be used to steal their identities.

Facebook users should become a fan of its security page at **www.facebook.com/security**, which has posts related to all sorts of security issues, tips, resources, and other information. Of recent concern is Graph Search, a search feature started in January 2013. With it any user can type in your name and get personal information that you have not secured, your friends have seen and made public, and non-friends have generated or obtained from others.

Here are some common ways cyber scammers exploit social media connections. Others are listed on the page entitled *Internet Social Networking Risks* on the FBI website at **www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks**.

- Clickjacking. Hyperlinks are concealed under legitimate-looking clickable content. Clicking on what looks like a Facebook "like" or "share" button actually downloads malware that can allow direct access to your computer or mobile device.
- Quizzes. Most people like online quizzes. Cyber crooks like them too. After completing the quiz and entering in your personal information and cell number, you notice your cell phone bill has an unauthorized charge on it.
- Phishing requests. An e-mail lures you to a fake Facebook, LinkedIn, or Twitter page, where you enter your login. As a result, the cybercriminal now has your account information.
- Shortened URLs. Clicking on shortened links, which are often used on social media sites, can unknowingly direct you to a website that installs malware on your computer.
- Suspicious e-mails. These scams involve e-mails luring you to go to your social media account. Some examples of bait are free products or gift cards, celebrity gossip, free apps, extra storage for your e-mail account, or a security issue fix. Once you've clicked on the link you've exposed your computer or mobile device to malware.
- Following with ill intent. Burglars may use Twitter to follow your tweets. For example, if you announce you're not home, it's the perfect time for a burglar to know when to break in.

To avoid problems on social networks or anywhere in the Internet, users should:

- Choose your network carefully. Make sure you understand its privacy settings and find out if it monitors the content of postings.
- Be careful about installing extras. Many third-party applications let you do more with your personal page but criminals sometime use them to steal personal information.
- Read your network's privacy policy regularly to stay informed on how it uses or discloses your information. Choose to opt out of information sharing wherever possible.
- Customize your personal privacy settings so only your friends have access to the information you post. Default settings on many sites allow anyone to see information about you. Check your settings frequently because they could be compromised when the site is updated, e.g., when new features are added.
- Type the address of your site directly into your browser or put it in your list of favorites. Don't click on a link to your site on an e-mail message or another website because you might be entering account information into a fake site where your personal information could be stolen.
- Never post any information that you don't want made public. Even if it's available only to "friends" you have no control over what a "friend" does with it. You can't retract or delete it after it's copied from your site.
- Untag yourself from pictures and other information you share with friends.
- Remember all password questions you have used to log into another website or account in case you forget your password. Never post information that contains the answers. And remember information you have posted so you don't create password questions that a hacker can get the answers to.
- Never post any information that might make you or your property vulnerable, e.g., your address or travel plans, or attractive to a burglar, e.g., pictures of valuable artwork or electronics.
- Wait until you get home to post your vacation blog and photos. Remove geotags with a metadata removal tool if you publish photos on the Internet while you are away. Even better, turn off the geotagging feature on your smartphone.
- Don't click on any links, videos, programs, etc. provided in messages, even if a "friend" encourages you to click on them. Treat links in messages like those in e-mails.
- Get program updates from the company's website, not through a provided link.

- Scan your computer regularly with updated anti-virus programs.
- Know who your friends are and be careful about accepting and adding new ones. Be very cautious about revealing information about yourself if you chat with people you don't know. Identity thieves might create a false profile to get information from you.
- Avoid giving away your "friends" e-mail addresses and don't allow any social networking services to scan your e-mail address book.
- Be suspicious of anyone, even a "friend," who asks for money over the Internet.

Fake Websites

Cybercriminals are now creating fake websites that will receive high search-engine rankings and thus attract the attention of persons searching for information on a particular subject. Persons just visiting those sites risk having their computers infected with malware. And if they click on any links in those sites they risk becoming a victim of identity theft and various scams, e.g., ones that claim you can make a lot of money for a small initial investment. To avoid these problems users should:

- Keep your computer's anti-virus systems up to date with the latest firewalls and software.
- Use caution clicking on links that claim to provide videos or information on hot topics in the current news, e.g., the earthquakes in Haiti and Chile. And be aware that the bad guys are now tricking Google into telling you that the link is a PDF file, which makes it look more authentic.
- Don't click on links to other websites. Look up the address elsewhere and retype it into your browser.
- Check to see where you would actually go before you click on a link. You can do this by scrolling your mouse over the link and reading the address in the box that will pop up over the link. Don't click on the link if this address does not match the one in the link.
- Use the tips provided above to counter phishing.

Do the following to make sure a website is legitimate and not selling counterfeit goods, especially if you are planning to buy a name-brand product. Always remember that if the price seems too good to be true, it probably is.

- Don't ever buy an item that you learn about via spam.
- Check that the domain name is spelled correctly. Cyber criminals are known to engage in type- or cyber-squatting to lure unsuspected victims to fake websites where they try to obtain personal and financial information or install malware on the victim's computer. They would use a name Appple.com or Bestbuyh.com. The fake website would be designed to look like the real one. It might offer a discount coupon in exchange for personal information or a credit card number.
- Check that the domain name ends in **.com**, **.org**, or **.net**. Those ending in **.cn** for China or **.mn** for Mongolia are likely to be fakes.
- Check the logo and picture of the product, and the spelling and contact information on the website.
- Call the phone number posted and talk to a live person. Ask where the product can be seen and visit the store.
- Don't conduct business with an anonymous seller.
- Save copies of all e-mails and other documents involved in the transaction. Then if you discover that an item is counterfeit you have documentation to use in reporting the crime to the National Intellectual Property Rights Coordination Center (IPR Center) at **www.iprcenter.gov/referral**. It coordinates the activities of various U.S. government agencies in conducting investigations related to intellectual property.

During open enrollment for health insurance under the Affordable Care Act (ACA), commonly called Obamacare, scammers have created fake websites to make consumers think they are the official federal or state websites and thereby secure bank account routing numbers for automatic monthly payments and other personal identifying information for malicious use. The official federal website is **www.healthcare.gov**. The official one for California is **www.coveredca.com**. Go directly to these websites for information and plan enrollment. And do not click on any links to health insurance exchanges that you might get in an e-mail or find in an Internet search.

E-card Dangers

You receive an e-mail saying "A friend has sent you an e-card." The e-mail appears to be from a legitimate card company, but malware is downloaded into your computer when you click the link to see the card. You should delete the e-mail if you don't recognize the sender or if you are instructed to download an executable program to view the e–card. And make sure your computer has adequate anti-virus protection. But even if you recognize the sender your computer could be harmed if the incoming e-mail is phony and you click on a link to an e-card or open an attachment. This happened around Christmas time in 2010 when employees of various government agencies received phony holiday messages that appeared to come from the White House.

Unsafe Drugs and Fraud by Online Pharmacies

Buying prescription drugs on the Internet is easy but finding a safe source is not. There are thousands of Internet drug outlets selling low-price prescription medications that may be counterfeit, contaminated, or otherwise unsafe. Many of these outlets are located outside the United States, don't require a valid prescription, offer foreign drugs or ones not approved by the U.S. Food and Drug Administration, have unsecure websites, don't provide a way to contact a licensed pharmacist by phone to answer questions, and don't comply with state and federal laws and/or the patient safety and pharmacy practice standards of the National Association of Boards of Pharmacy (NABP).

You can avoid the risks of dealing with these rogue websites, which constitute about 96 percent of those on the Internet, by using safe sources have been identified by the NABP in its Verified Internet Pharmacy Practice Sites (VIPPS) program. They are listed as Recommended Internet Pharmacies on its website at www.nabp.net. These sites have undergone and successfully completed the NABP's accreditation process that includes a review of all policies and procedures regarding the practice of pharmacy and dispensing of medicine over the Internet as well as an on-site inspection of facilities used by the site of receive, review, and dispense medicine. The NABP website also lists Not Recommended Internet pharmacies and sites that have received its e-Advertiser Approval. These sites offer only limited pharmacy services or other prescription drug-related services. They have also been found to be safe, reliable, and lawful.

Some online pharmacies only exist to obtain personal information and membership fees. Their e-mail ads offer a large variety of scheduled drugs without a prescription to members only. If you join you lose your membership fee and become vulnerable to identity theft.

Hacked E-mail

You might have been hacked if:

- People in your address book write that they are getting e-mails you didn't send. They might have seemingly random links or urgent pleas to wire money.
- Your sent-message folder has messages you didn't send, or it has been emptied.
- Your social media accounts have posts you didn't make.
- You can't log onto your e-mail or social media accounts.

Do the following if you've been hacked.

- Make sure you have security software and it's up to date. Install it if you don't have it. Only buy it from a reputable, well-known company.
- Run your security software to scan your computer for viruses and malware. Then delete any suspicious software and restart your computer.
- Set your security software, internet browser, and operating system to update automatically with the latest patches.
- Change your passwords. Make them strong so they will be hard to guess. If you use similar passwords for other accounts, change them too.
- Get advice your e-mail provider or social networking site about restoring your account. If your account has been taken over you might need to fill out forms to prove it's really you trying to get back into your account.

- Check your account settings. Make sure your signature and away messages don't contain unfamiliar links, and that messages aren't being forwarded to someone else's address. On your social networking service look for changes to the account since you last logged in, say a new "friend."
- Send an e-mail to people in your address book to let them know you've been hacked. Warn them about possible malicious links or fake pleas for money. Put their e-mail addresses in the Bcc: line to keep them hidden.

Do the following to prevent being hacked:

- Use strong, unique passwords for important sites, especially your financial accounts.
- Safeguard your usernames and passwords. Never provide them in response to an e-mail.
- Use multi-factor authentication if possible.
- Don't click on links or open attachments in e-mails unless you trust them. And don't forward random links.
- Download free software only from sites you know and trust.
- Don't treat public computers like your personal computer. And be careful any time you use public Wi-Fi.

SAFER USE OF THE INTERNET

Many U.S. Government agencies are involved in promoting safe cyber practices. The main ones are the DHS and the FTC. Four of their programs are described below.

National Cyber Awareness System

Persons with specific concerns about cybersecurity should visit the US-CERT's website at **www.us-cert.gov**. US-CERT leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. Its National Cyber Awareness System offers a variety of information for users with varied technical expertise. Those with more technical interest can read or subscribe to the Alerts, Current Activity Updates, or Bulletins. Those looking for more general-interest pieces can read the Tips. Current Activity Updates provide timely information on security risks to help you better protect your systems from malware campaigns and mitigate new software vulnerabilities. It is updated frequently and typically contains less detail than Alerts, which warn about vulnerabilities, incidents, and other security issues that pose major risks. Bulletins provide weekly summaries of new vulnerabilities with patch information provided when available. Tips provide advice about common security issues for home and business users. They deal with general security, attacks and threats, e-mail and communication, mobile devices, privacy, safe browsing, software, and applications.

You can take the following to protect your privacy and personal information.

- Do business with credible companies. Before supplying any personal information online, consider the answers to the following questions: Do you trust the business? Is it an established organization with a credible reputation? Does the information on the site suggest that there is a concern for the privacy of user information? Is there legitimate contact information provided?
- Limit cookies to make sure that other sites are not collecting personal information about you without your knowledge. Choose to allow cookies only for the website you are visiting, and block or limit cookies from a third-party. Make sure that cookies are disabled if you are using a public computer.
- Don't use your primary e-mail address in online submissions. Submitting your e-mail address could result in spam. Consider opening an additional e-mail account for use online if you don't want your primary e-mail account flooded with unwanted messages. Make sure to log onto the account on a regular basis in case the vendor sends information about changes to policies.
- Avoid submitting credit card information online. Some companies offer a phone number you can use to provide your credit card information. Although this does not guarantee that the information will not be compromised, it eliminates the possibility that attackers will be able to hijack it during the submission process.
- Take advantage of options to limit exposure of personal information. Default options on certain websites may be chosen for convenience, not for security. For example, avoid allowing a website to remember your password. If your password is stored, your profile and any account information you have provided on that site is readily available if an attacker gains access to your computer. Also evaluate your settings on websites used for social

networking. The nature of those sites is to share information, but you can restrict access to certain information so that you limit who can see what.

As of July 1, 2016 the following documents were available on the US-CERT website at **www.us-cert.gov/security-publications**. They can help you with everything from setting up your first computer to understanding the nuances of emerging threats.

- General Internet Security
  - The Risks of Using Portable Devices
  - Cyber Threats to Mobile Phones
  - Understanding and Protecting Yourself Against Money Mule Schemes
  - Socializing Securely: Using Social Networking Services
  - Understanding Voice over Internet Protocol (VoIP)
  - Banking Securely Online
  - Playing it Safe: Avoiding Online Gaming Risks
  - Protecting Aggregated Data
  - Introduction to Information Security
  - Password Security, Protection, and Management
  - South Korean Malware Attack
- Securing Your Computer
  - Securing Your Web Browser
  - Software License Agreements: Ignore at Your Own Risk
  - Spyware
  - Using Wireless Technology Securely
  - Virus Basics
  - Data Backup Options
  - Disposing of Devices Safely
  - Common Risks of Using Business Apps in the Cloud
  - The Basics of Cloud Computing
  - Small Office/Home Office Router Security
  - Governing for Enterprise Security
  - Home Network Security
  - Recognizing and Avoiding E-mail Scams
- Recovering from an Attack
  - Recovering from a Trojan Horse or Virus
- Distributable Materials
  - Protect Your Workforce Campaign
  - Cybersecurity: What Every CEO Should Be Asking
  - NCCIC Cyber Incident Scoring System
- Technical Publications
  - Computer Forensics
  - The Continuing Denial of Service Threat Posed by DNS Recursion (v2.0)
  - Malware Threats and Mitigation Strategies
  - Malware Tunneling in IPv6
  - National Strategy to Secure Cyberspace
  - Technical Trends in Phishing Attacks
  - DHS Cyber Security Initiatives
  - Fundamental Filtering of IPv6 Network Traffic
  - Practical Identification of SQL Injection Vulnerabilities
  - Website Security
  - DDoS Quick Guide
  - "Heartbleed" Open SSL Vulnerability
  - Technical Information Paper: Coreflood Trojan Botnet
  - Combating the Insider Threat
  - System Integrity Best Practices

- Keylogger Malware in Hotel Business Centers
- Cyber Threats to Mobile Devices
- Backoff Point-of-Sale Malware
- SQL Injection

Stop.Think.Connect

In 2009 President Obama recognized the need to increase education and dialogue about cybersecurity and issued the Cyberspace Policy Review, which became the blueprint for cybersecurity in the future. In this review the DHS was asked to create an ongoing cybersecurity awareness campaign. It was called Stop.Think.Connect and was launched in October 2010. It provides tips and resources for cybersecurity on its website at **www.dhs.gov/stopthinkconnect**. They include the following.

Before you use the Internet take time to understand the risks and learn how to spot potential problems.

- Stop hackers from accessing your accounts, set secure passwords.
- Stop posting and sharing too much, keep your personal information personal.
- Stop doing something if it doesn't feel right, trust your gut.
- Stop questionable online behavior, only do and say things online that you would do in real life.

Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact the safety of yourself and your family.

- Think about the information you want to share before you share it.
- Think how your online actions can affect your offline life.
- Think before you act, don't automatically click on links.
- Think about why you are sharing information online. Is it going to be safe?
- Think about why you're going to a website. Did you get it from someone you trust?
- Think **a**bout who you're talking to online. Do you *really* know who they are?

Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

- Connect over secure networks.
- Connect with people you know and trust.
- Connect with care and be on the lookout for potential threats.
- Connect safely and show your friends and family how to behave online.
- Connect with websites you trust.

The following tips come from **www.stopthinkconnect.org**.

Keep a clean machine:

- Have the latest security software, web browser, and operating system.
- Use programs that automatically connect and update your security software.
- Protect all devices that connect to the Internet from all malware.
- Set up local administrator accounts on your computing devices so only an administrator (you) can download programs and applications. Then only download from a trusted source. If you have any questions about the legitimacy of a site, don't download from it.
- Use your security software to scan all USBs and other external devices before attaching them to your computer.

Protect your personal information:

- Secure your accounts with unique, strong passwords that have more than eight characters with at least one capital letter, one lowercase letter, one number, and one symbol.
- Keep a list of your passwords stored in a safe place away from your computer.
- Use privacy and security settings to limit who you share information with.

Connect with care:

- Delete any suspicious e-mail, tweets, posts, and online advertising. When in doubt, throw it out.
- Limit the business you conduct from Wi-Fi hotspots and adjust your security settings to limit who can access your computer.
- Secure your home wireless network. The minimum level of encryption is WPA2. Replace your router if it can't run WPA2. Protect your router with a strong password. The following website has good information on wireless routers: **www.onguardonline.gov/articles/0013-securing-your-wireless-network**.
- Use only secure websites when banking and shopping, i.e., ones with **https://** or **shttp://** in their addresses.

Be web wise:

- Keep pace with new ways to stay safe online by checking trusted website for the latest information.
- Think before you act when you are implored to act immediately, offered something that sounds too good to be true, or asked for personal information.
- Back up your valuable information by making an electronic copy and storing it in a safe place.

Be a good online citizen:

- Practice good online safety habits.
- Post about others as you would have them post about you.
- Report all types of cybercrime to you local law enforcement agency and other appropriate authorities.

OnGuardOnline.gov

The FTC manages this website in partnership with the DHS in its Stop.Think.Connect campaign, and many other federal agencies. Its website, **www.OnGuardOnline.gov**, provides practical tips from the federal government to help you guard against internet fraud, avoid scams, secure your computers, protect your privacy, protect your kids online, be smart online, etc.

Stop.Think.Click

This effort defines seven practices for safer computing and provides tips on preventing identity theft, safe use of social networking sites, online shopping, Internet auctions, avoiding scams, and wireless security. It also provides a glossary of terms. The seven practices are:

1. Protecting your personal information
2. Knowing who you're dealing with
3. Using anti-virus software as well as a firewall
4. Setting up your operating system and web browser software properly, and updating them regularly
5. Protecting your passwords
6. Backing up your important files
7. Learning who to contact if something goes wrong online.